1 fw AF

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200314543-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Michael F. Angelo et al.

Confirmation No.: 2632

Application No.: 10/764,918

Examiner: Doan, Duc T.

Filing Date: January 26, 2004

Group Art Unit: 2188

Title: Method and Apparatus for Operating Multiple Security Modules

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 12-21-2007.

☒ The fee for filing this Appeal Brief is $510.00 (37 CFR 41.20).

☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $460	☐ 3rd Month $1050	☐ 4th Month $1640

☐ The extension fee has already been filed in this application.

☐ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 510. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.

☒ I hereby certify, that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: February 20, 2008

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.
Date of facsimile:
Typed Name: Jeanna Reed
Signature: Jeanna Reed

Respectfully submitted,
Michael F. Angelo et al.
By _____
Michael G. Fletcher
Attorney/Agent for Applicant(s)
Reg No. : 32,777
Date : February 20, 2008
Telephone : (281) 970-4545

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Michael F. Angelo et al.	§	Confirmation No.: 2632	
	§		
	§	Group Art Unit: 2188	
Serial No.: 10/764,918	§		
	§	Examiner: Doan, Duc T.	
Filed: January 26, 2004	§		
	§		
For: Method and Apparatus for Operating Multiple Security Modules	§	Atty. Docket: NUHP:0210 200314543-1	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF TRANSMISSION OR MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted by facsimile to the United States Patent and Trademark Office in accordance with 37 C.F.R. § 1.6(d), or is being transmitted via the Office electronic filing system in accordance with 37 C.F.R. § 1.6(a)(4), or is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below:

February 20, 2008 — Date

Jeanna Reed

APPEAL BRIEF PURSUANT TO 37 C.F.R. §§ 41.31 AND 41.37

This Appeal Brief is being filed in furtherance to the Notice of Appeal mailed on December 21, 2007, and received by the Patent Office on December 21, 2007.

The Commissioner is authorized to charge the requisite fee of $510.00, and any additional fees which may be necessary to advance prosecution of the present application, to Account No. 08-2025; Order No. 200314543-1.

1. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, L.P. the Assignee of the above-referenced application by virtue of the Assignment recorded at reel 14937, frame 0082, and dated January 26, 2004. Accordingly, Hewlett-Packard Development Company, L.P., as the parent company of the Assignee of the above-referenced application, will be directly affected by the Board's decision in the pending appeal.

2. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any other appeals or interferences related to this Appeal. The undersigned is Appellants' legal representative in this Appeal.

3. STATUS OF CLAIMS

Claims 1-28 and 31-34 are currently pending. Claims 27 and 28 have been previously allowed and claims 29 and 30 have been previously cancelled. Claims 1-26 and 31-34 are currently under final rejection and, thus, are the subject of this Appeal.

4. STATUS OF AMENDMENTS

As the instant claims have not been amended at any time, there are no outstanding amendments to be considered by the Board.

5. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates generally to security modules and a method of operating the security modules in a computer. *See* specification, page 30, lines 2-3. The Application contains six independent claims, namely, claims 1, 8, 14, 21, 27, and 31. Except for claim 27, which has been allowed, all of the independent claims are the subject of this Appeal. The subject matter of the claims presented in this appeal is summarized below.

With regard to the aspect of the invention set forth in independent claim 1, discussions of the recited features of claim 1 can be found at least in the below cited locations of the specification and drawings. By way of example, claim 1 generally recites a method of operating a first security module in a computer. *See, e.g.,* Figs. 3-6; specification, page 9, lines 2-5; page 14 line 10 through page 16, lines 15. The method includes the act of detecting a second security module in the computer, wherein the second security module is configured to perform the same functions as the first security module. *Id.* at Figs. 3-6; page 14, lines 7-12; page 11, lines 9-12; page 15, lines 1-13. Additionally, the method includes the act of determining whether a key associated with

the second security module is stored at the first security module; and obtaining the key associated with the second security module if the key associated with the second security module is not stored at the first security module. *Id.* at Fig. 6; page 15, lines 15 through page 16, line 15.

With regard to the aspect of the invention set forth in independent claim 8, discussions of the recited features of claim 8 can be found at least in the below cited locations of the specification and drawings. By way of example, claim 8 generally recites a first security module in a computer. *See, e.g.,* Fig. 3; specification, page 8, line 21 through page 9, line 5. The first security module includes a detector that is adapted to detect another security module configured to perform the same functions as the first security module in the computer and determine whether one of a plurality of keys stored at the first security module is associated with the other security module. *Id.* at Figs. 1 and 3; page 7, line 22 through page 8, line 19; page 11, lines 9-12; page 15, line 1 through page 16, line 5. Additionally, the first security module includes a device that obtains at least one key associated with the other security module if the one of the plurality of keys stored at the first security module is not associated with the other security module. *Id.*

With regard to the aspect of the invention set forth in independent claim 14, discussions of the recited features of claim 14 can be found at least in the below cited locations of the specification and drawings. By way of example, claim 14 generally recites a first security module in a computer that includes means for detecting another security module in the computer, wherein the other security module is configured to perform the same functions as the first security module. *See, e.g.,* Figs. 2 and 3; page 7, line 22 through page 8, line 19; page 11, lines 9-12; page 15, line 1 through page 16, line 5. The first security module also includes means for determining whether a key associated with the other security module is stored at the first security module. *Id.* Additionally, the first security module includes means for obtaining the key associated

with the other security module if the key associated with the other security module is not stored at the first security module. *Id.*

With regard to the aspect of the invention set forth in independent claim 21, discussions of the recited features of claim 21 can be found at least in the below cited locations of the specification and drawings. By way of example, claim 21 generally recites a computer including a processor configured to execute program instructions and a storage device configured to store program instructions to be delivered to the processor. *See, e.g.,* Fig. 3, specification, page 9, lines 7-17. The computer also includes a first security module and a second security module, wherein the second security module is configured to perform the same functions as the first security module. *Id.* at Fig. 3; page 8, line 21 through page 9, line 5; page 10, lines 19-25; page 11, lines 9-12;. The first security module includes a detector adapted to detect the second security module and determine whether one of a plurality of keys stored at the first security module is associated with the second security module. *Id.* at Fig. 2; page 8, lines 2-19; page 15, lines 1-13. The first security module obtains at least one key associated with the second security module if one of the plurality of keys stored at the first security module is not associated with the second security module. *Id.* at Figs. 5 and 6; page 15, line 15 through page 16, line 5.

With regard to the aspect of the invention set forth in independent claim 31, discussions of the recited features of claim 31 can be found at least in the below cited locations of the specification and drawings. By way of example, claim 31 generally recites a computer network including a plurality of computers and a network infrastructure that connects the plurality of computers together. *See, e.g.*, Fig. 1; specification, page 6, line 12 through 7, line 20. At least one of the plurality of computers comprises a first security module and a second security module, wherein the second security module is configured to perform the same functions as the first security module. *Id.* at Fig. 3, page 8, lines 21-22; page 10, lines 19-23; page 11, lines 9-12. The

first security module includes a detector adapted to detect the second security module and determine whether a key associated with the second security module is stored at the first security module. *Id.* at Figs. 5 and 6; page 15, line 1 through page 16, line 5; page 17, line 1 through page 18, line 18. The first security module obtains the key associated with the second security module if the key associated with the second security module is not stored at the first security module. *Id.*

A benefit of the invention, as recited in these claims, is the ability to provide fault tolerance, and enhance security and reliability of computer systems. *See* specification, page 8, lines 18-19. This is a clear difference and distinction from the prior art, as discussed below.

6. **GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

First Ground of Rejection for Review on Appeal:

Appellants respectfully urge the Board to review and reverse the Examiner's first ground of rejection in which the Examiner rejected claims 8-13 and 14-20 under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter.

Second Ground of Rejection for Review on Appeal:

Appellants respectfully urge the Board to review and reverse the Examiner's second ground of rejection in which the Examiner rejected claims 1-26, 31, and 32 under 35 U.S.C. § 103(a) as being unpatentable over Appellants' admitted prior art (APA) and in view of Challener, U.S. Publication No. 2003/0174842 (hereinafter "Challener").

Third Ground of Rejection for Review on Appeal:

Appellants respectfully urge the Board to review and reverse the Examiner's third ground of rejection in which the Examiner rejected claims 33 and 34 under 35 U.S.C. § 103(a) as being unpatentable over APA and Challener as applied to claims 1 and 8

respectively, and in view of Dickinson et al., U.S. Patent No. 7,187,771 (hereinafter "Dickinson").

7. ARGUMENT

As discussed in detail below, the Examiner has improperly rejected the pending claims. Further, the Examiner has misapplied long-standing and binding legal precedents and principles in rejecting the claims under Section 103. Accordingly, Appellants respectfully request full and favorable consideration by the Board, as Appellants strongly believe that claims 1-28 and 31-34 are currently in condition for allowance.

A. Ground of Rejection No. 1:

The Examiner rejected claims 8-13 and 14-20 under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Specifically, the Examiner stated:

> Claims 8-13, 14-20 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.
>
> Claim 8, 14 direct to a security module which is a software/program (see specification's paragraph 21). Therefore, the claimed invention is directed to non-statutory subject matter.
>
> All dependent claims are rejected as having the same deficiencies as the claims they depend from.

Office Action, pages 2-3. Appellants respectfully traverse the rejection.

Legal Precedent

According to the Supreme Court, Congress intended statutory subject matter to "include anything under the sun that is made by man." *Diamond v. Chakrabarty*, 447 U.S. 303, 308-09; 206 U.S.P.Q. 193, 197 (1980). Indeed, exclusions of statutory subject matter are limited to laws of nature, natural phenomena and abstract ideas. *See Diamond v. Diehr*, 450 U.S. 175, 185; 209 U.S.P.Q. 1, 7 (1981). Other than these specific

exceptions, therefore, nearly anything man made is statutorily patentable subject matter under 35 U.S.C. §101.

With particular regard to software or programs, if they are in a tangible medium, they are considered patentable subject matter under Section 101. *See In re Beauregard,* 53 F.3d 1583 (Fed Cir. 1995). Indeed, the Commissioner of Patents stated, "[C]omputer programs embodied in a tangible medium...are patentable subject matter under 35 U.S.C. §101." *Id.* Moreover, when functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. M.P.E.P. § 2106.01.; *See In re Lowry,* 32 F.3d 1579, 1583-84 (Fed. Cir. 1994).

Appellants respectfully assert that claims 8 and 14 are directed to statutory subject matter under Section 101, as they are directed to apparatuses and recite discrete physical structures. In particular, independent claims 8 and 14 are each directed to "[a] first security module in a computer" and recite discrete physical structures in the bodies of the respective claims. Specifically, the body of claim 8 recites, "*a detector* that is adapted to detect another security module...and *a device* that obtains at least one key." (Emphasis added). The body of claim 14 recites, "*means for detecting* another security module...*means for determining* whether a key associated with the other security module is stored at the first security module; and *means for obtaining* the key." (Emphasis added). Moreover, the specification clearly describes the security modules as including physical structure. *See, e.g.*, FIG. 3; paragraph 28, lines 3-4 (stating "the first TPM 143 may include an input/output interface, a *processor*, and a *memory* 156 that is used to store TPM keys 158" (Emphasis added)). Accordingly, the subject matter of independent claims 8 and 14 clearly contemplated to include tangible hardware elements, as well as software.

The Examiner's rejection seems based on a presumption that, because certain elements of the claimsed invention may be interpreted as comprising software, that independent claims 8 and 14, and the claims dependent thereon, are non-statutory. This presumption is simply not correct. As mentioned above, the Commissioner of Patents has recognized the patentability of software, provided that it is embodied in a tangible medium. *See In re Beauregard,* 53 F.3d 1583 (Fed Cir. 1995). It is clear from the specification that, to the extent the claimed security modules comprise software, the security modules are intended to be implemented in a tangible medium. In particular, the specification describes a first security module that includes NVRAM 140 (FIG. 3) and a second security module that includes a memory 160 (FIG. 3). Those of ordinary skill in the art would clearly recognize the NVRAM 140 and the memory 160 as tangible computer readable media. Because the specification clearly supports the software implementation of security modules in a tangible machine-readable medium, the independent claims are statutory subject matter.

In summary, Appellants respectfully assert that independent claims 8 and 14 are statutory because they are directed to either physical apparatuses or software that is stored on a tangible computer readable medium. As such, Appellants respectfully request withdrawal of the rejection of independent claims 8 and 14, as well as the rejection of all claims dependent thereon, under 35 U.S.C. § 101.

B. **Ground of Rejection No. 2:**

The Examiner rejected claims 1-26, 31, and 32 under 35 U.S.C. § 103(a) as being unpatentable over APA and in view of Challener. Specifically, with respect to claim 1, the Examiner stated:

> As in claim 1, APA discloses a method of operating security modules in a computer including having a first security module and a second security module both of them are configured to perform the same functions, that is the functions associating with a security module (APA's paragraph 4, two security modules configured to perform

> the same secutiry functions such as encrypting, sealing etc..).
>
> APA does not disclose the claim's details associating with the keys of security modules, However, Challener '842 describes a method for storing private key of one security in another security module using establish standard such as TCPA (Challener's paragraph 6, lines 1-10) comprising the acts of: detecting a second security module in the computer; determining whether a key associated with the second security module is available to the first security module (Challener '842's paragraph 28, Fig 3: #54 query whether user's private key is stored on the TCM server, Fig. 1: #40 that corresponds to the claim's first security module); and obtaining the key associated with the second security module if the key associated with the second security module is not stored at the first security module (Challener '842's paragraph 28, server obtains the private key from the client's security module, Fig. 1: #54 that corresponds to the claim's second security module, Fig. 1: #22; Challener's paragraph 12 discloses that the first security module, TCM server Fig. 1: #40, obtaining the private key associating with the second security module Fig. 1: #22, and providing this key information to a client/user. Obviously, if this key has not been stored at the first security module, the first security module, server, will obtain it from the client's computer and save it for future referencing, in a migrating manner, see Fig. 4a, and paragraph 32.)
>
> It would have been obvious to one of ordinary skill in the art at the time of invention to include the method and associating apparatus for storing private key of one security in another security module using establish standard such as TCPA in APA's system, thereby the private key or one security module can be retrieved from another security safely with any computers enable with established standard such as TCPA (see Challener's paragraph 8.

Office Action, page 3-4. The Examiner indicated that claims 8, 14, 21 and 31 were rejected based on the same rationale as in the rejection of claim 1. Office Action, page 6. Appellants respectfully traverse the rejection

Legal Precedent

The burden of establishing a *prima facie* case of obviousness falls on the Examiner. *Ex parte Wolters and Kuypers*, 214 U.S.P.Q. 735 (B.P.A.I. 1979). To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 180 U.S.P.Q. 580 (C.C.P.A. 1974). However, it is not enough to show that all the elements exist in the prior art since a claimed invention composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. *KSR International Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007). It is important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. *Id.* Specifically, there must be some articulated reasoning with a rational underpinning to support a conclusion of obviousness; a conclusory statement will not suffice. *In re Kahn,* 441 F.3d 977, 988 (Fed. Cir. 2006). Indeed, the factual inquiry determining whether to combine references must be thorough and searching, and it must be based on *objective evidence of record. In re Lee,* 61 U.S.P.Q.2d 1430, 1436 (Fed. Cir. 2002).

Additionally, Appellant submits that, during patent examination, the pending claims must be given an interpretation that is *reasonable* and *consistent* with the specification. *See In re Prater*, 162 U.S.P.Q. 541, 550-51 (C.C.P.A. 1969); *In re Morris*, 44 U.S.P.Q.2d 1023, 1027-28 (Fed. Cir. 1997); *see also* M.P.E.P. § 2111 (describing the standards for claim interpretation during prosecution). Indeed, the *specification* is "the primary basis for construing the claims." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (citations omitted). It is usually dispositive. *See id.* Interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach. *See In re Cortright*, 49 U.S.P.Q.2d 1464, 1468 (Fed. Cir. 1999); *see also* M.P.E.P. § 2111. That is, recitations of a claim must be read as they would be interpreted by those of ordinary skill in the art. *See Rexnord Corp. v. Laliram Corp.*, 60 U.S.P.Q.2d 1851, 1854 (Fed. Cir. 2001); *see also* M.P.E.P. § 2111.01. In summary, an Examiner, during

prosecution, must interpret a claim recitation as one of ordinary skill in the art would reasonably interpret the claim in view of the specification. *See In re American Academy of Science Tech Center,* 70 U.S.P.Q.2d 1827 (Fed. Cir. 2004).

Independent Claims 1, 8, 14, 21 and 31

The present application is directed to techniques for operating multiple security modules, such as trusted platform modules ("TPMs"), in a *single* computer system. *See* specification, paragraphs 3, 4 and 16. In addition to other benefits, such as maintenance of system integrity, the operation of multiple TPMs within a single computer system may provide redundancy of keys to permit continued system operation in the event that one security module is inoperable. *Id.* at 33 and34. As such, independent claim 1 recites, *inter alia*, a method of operating a first security module in a computer comprising "detecting a second security module *in the computer*, wherein *the second security module is configured to perform the same functions as the first security module*." (Emphasis added). Independent claim 8 recites, *inter alia,* a first security module comprising "a detector that is adapted to detect another security module *configured to perform the same functions as the first security module in the computer*." (Emphasis added). Independent claim 14 recites, *inter alia,* a first security module comprising "means for detecting another security module *in the computer*, wherein *the other security module is configured to perform the same functions as the first security module*." (Emphasis added). Independent claims 21 and 31 both recite, *inter alia,* a computer comprising "a first security module; and a second security module, wherein *the second security module is configured to perform the same functions as the first security module*." (Emphasis added).

In sharp contrast, the Challener reference does not disclose multiple security modules in a *single* computer system, much less multiple security modules configured to perform the same functions in a computer system. The Challener reference is directed to a system that allows for private key migration *between computers* in a network environment. *See* Challener, paragraph 28. The sharing of the private key is useful in a free seating

network environment to allow a user to authenticate at different client computers attached to the network without needing additional hardware. *Id.* at paragraph 35. The creation, storing, and sharing of the private keys is accomplished by TPMs in the client and server computers, respectively. *Id.* at Fig. 1; paragraphs 24, 26 and 27. As such, the Challenger reference discloses modules being located in *two separate and distinct computers* (the client and the sever). *Id.* at Fig. 1. However, the Challener reference does not disclose, teach, suggest or provide any motivation with respect to providing *multiple security modules in the same computer*, much less wherein the modules are configured to perform the same functions. As such, for at least this reason, the Challener reference fails to disclose all of the features set forth in the independent claims 1, 8, 14, 21 and 31.

Appellants respectfully assert that the portion of the instant application to which the Examiner cites as "Applicant's admitted prior art (APA)" in rejecting claims 1, 8, 14, 21 and 31 does not qualify as prior art nor can be considered an admission of such. In particular, the section of the specification in which the portion cited by the Examiner is located is prefaced with the following statement:

> This section is intended to introduce the reader to various *aspects of art, which may be related to various aspects of the present invention that are described and/or claimed below*. This discussion is believed to be helpful in providing the reader with background information to facilitate a better understanding of the various aspects of the present invention. Accordingly, *it should be understood that these statements are to be read in this light, and not as admissions of prior art.*

Specification, page 2, lines 5-10. (Emphasis added). Accordingly, Appellants respectfully assert that the statements upon which the Examiner relied in the Section 103 rejection cannot be used in combination with the Challener reference as they are presented simply to facilitate understanding of the aspects of the present invention and Appellants have specifically stated that these statements are *not* admissions of prior art. Furthermore, Appellants respectfully assert that the fact that the Examiner is unable to

find any reference, other than the instant application, which disclose the features recited in the claims indicates that it is *not* prior art. As such, for at least these reasons, Appellants respectfully assert that a *prima facie* case for obviousness has not been presented with respect to claims 1, 8, 14, 21 and 31.

Moreover, even if the portions of the instant application which were cited by the Examiner were considered to be prior art, a *prima facie* case of obviousness has not been presented. Specifically, while the portion of the instant application cited by the Examiner discloses two security modules in a computer system, it does not disclose that they are configured to perform the same functions. Furthermore, the Challener reference fails to disclose this feature. In particular, the Challener reference discloses a system wherein two security modules in two different computers perform different functions. For example, one security module located in the server is configured to collect keys from and distribute keys to client computers, while a second security module located in a client computer may generate keys, provide keys to the security module of the sever and access the keys stored at the server to allow for the free-seating of a user within the network environment. *See* Challener, paragraphs 11 and 12. As such, not only are the security modules in separate computers, but they do not perform the same functions.

For at least the reasons set forth above, Appellants respectfully assert that the Examiner has failed to present a *prima facie* case for obviousness under Section 103. Specifically, because the cited portions of the instant application cannot be used as prior art or as admissions of prior art, and because the Challener reference fails to disclose all the features of independent claims 1, 8, 14, 21 and 31, a *prima facie* case for obviousness has not been made. Accordingly, Appellants respectfully request reversal of the rejection under Section 103 of claims 1, 8, 14, 21 and 31, as well as all claims depending therefrom.

Claims 5, 12, 18 and 25

Appellants respectfully assert that claims 5, 12, 18 and 25 are not only allowable based on their respective dependency from claims 1, 8, 14, and 21, but also for unique and non-obvious features recited therein. Specifically, claims 5, 12, 18 and 25 each set forth the sending of a "public key along with validation information" from the first security module to a the second (or other) security module if the key associated with the second (or other) security module is not stored at the first security module. Contrary to the Examiner's assertion, the Challener reference fails to disclose this feature.

In rejecting claims 5, 12, 18 and 25, the Examiner cited to paragraph 31 of the Challener reference which states in its entirety:

> In a preferred embodiment, migrating the user's private key to the server, as depicted in block 58, and requesting the user's private key from the server to a specific client computer, as described in block 62, must first be authorized by the client user. This authorization is preferably performed by transmitting authorization data using keyed-has message authentication code (HMAC), as described by Internet RFC 2104, HMAC, Keyed-Hashing for Message Authentication, and ANSI X9.71, Keyed Hash Message Authentication Code, herein incorporated by reference and well known to those skilled in the art of cryptology.

Challener, paragraph 31. As can be seen, the portion of the Challener reference cited by the Examiner does not even mention public keys, much less the sending of "public keys along with validation information," as set forth in claims 5, 12, 18 and 25. Indeed, paragraph 31 simply discloses that in the Challener system the migrating of a *private key* must be authorized. *See id.* The authorization is apparently sent independent of any keys. *See Id.* As such, Appeallants respectfully assert that the Challener reference fails to disclose all the features of claims 5, 12, 18 and 25. For this additional reason, Appellants respectfully request reversal of the Examiner's rejection under Section 103 and allowance of claims 5, 12, 18 and 25.

C. **Ground of Rejection No. 3:**

The Examiner rejected claims 33 and 34 under 35 U.S.C. § 103(a) as being unpatentable over APA and Challener as applied to claims 1 and 8 respectively, and in view of Dickinson. Specifically, the Examiner stated:

> As in claim 33 Challener further discloses comprising the act of accessing data encrypted by the second security module using the key associated with the second security module (Challener discloses a method in which at first secure module (Fig. 1: #40) can access data encrypted by the second security module using the key associated with second security module (Challener's Fig. 3: #60-64, paragraph 31, the stored private key (corresponding to the claim's data) is encrypted using non-migratable public key (corresponding to the claim's key associating with the second security module), and retuning the user's private key/data to the client). In other words, Challener teaches a method in which a first security module can retrieve data associating with the second security module by using the stored key associated with the second security module and presenting the data tot eh user. APA and Challener do not expressly disclose the aspect of the claim's regarding the failure of the second security module. However, Dickenson discloses a method in which important data is controlled by secure/trust module logic (see Abstract, Fig. 2). Dikinson further discloses that the secure trust engines (see Dickinson's column 5 lines 60-67, column 13line 46 to column 14 line 3, trust engines perform authenticate functions), which control several redundant copy of critical data, such that the failure of one module/one component would not affect the overall secure system.
>
> It would have been obvious to one of ordinary skill in the art at the time of the invention to include the redundant method for storing copies of data controlled by redundant secure/trusted modules in APA's system modified by Challener and thereby if one of the secure modules fails, the data can be obtained from the remaining secure modules or other copies of data (see Dickinson's column 17 lines 46-61).
>
> Claim 34 is rejected based on the same rationale.

Office Action, page 6-7. Appellants respectfully traverse this rejection.

Claims 33 and 34

As discussed above, the instant application is directed to techniques for operating multiple security modules, such as trusted platform modules ("TPMs"), in a *single* computer system. *See* specification, paragraphs 3, 4 and 16. In addition to other benefits, such as maintenance of system integrity, the operation of multiple TPMs within a single computer system may provide redundancy of keys to permit continued system operation in the event that one security module is inoperable. *Id.* at 33 and 34. As such, independent claim 1 recites, *inter alia*, a method of operating a first security module in a computer comprising "detecting a second security module *in the computer*, wherein *the second security module is configured to perform the same functions as the first security module*." (Emphasis added). Independent claim 8 recites, *inter alia,* a first security module comprising "a detector that is adapted to detect another security module *configured to perform the same functions as the first security module in the computer*." (Emphasis added).

Claims 33 and 34 depend from claims 1 and 8, respectively. Claim 33 recites, "The method set forth in claim 1, comprising the act of accessing data encrypted by the second security module using the key associated with the second security module if the second security module fails." Claim 34 recites, "The first security module set forth in claim 8, wherein the first security module is configured to decrypt data encrypted by the other security module if the other security module fails."

Appellants respectfully assert that Dickinson reference fails to overcome the deficiencies of the Challener reference with respect to claims 1 and 8. As discussed in detail above, the portion of the instant application cited by the Examiner cannot be used as prior art and the Challener reference fails to disclose multiple security modules in a single computer, much less multiple security modules configured to perform the same functions. The Dickinson reference fails to overcome these deficiencies.

The Dickinson reference is directed to a system that uses server centric keys for security purposes. *See* Dickinson, abstract; page 2, lines 34-43. Dickinson discloses a trust engine that stores keys and authentication data. *Id.* at Figs. 1 and 2 (110). The trust engine may be a plurality of trust engines which are geographically separated to increase security. *Id.* at col. 31, line 56 through col. 32, line 14. However, Appellants are unaware of, and the Examiner has not cited to, any portion of the Dickinson reference that can reasonably be considered to disclose multiple security modules in a single computer. As such, for at least this reason, the Appellants assert that the Dickinson reference fails to overcome the deficiencies of the Challener reference with respect to claims 1 and 8. Accordingly, Appellants respectfully assert that claims 33 and 34 are allowable based on their respective dependencies from claims 1 and 8.

Moreover, Appellants assert that the Dickinson reference does not disclose a first security module accessing data encrypted by the second or other security module if the second or other security module fails, as set forth in claims 33 and 34. Specifically, the Dickinson reference only discloses that each authentication engine has current data to compare and determine an authentication result. *See* Dickinson at col. 5, lines 60-67. This allows for quicker response time in the geographically distributed system (where the trust engines are remotely located from each other). *Id.* at col. 31, line 56 through col. 32, line 14. In the Dickinson reference, there is, however, no discussion of a first security module accessing data encrypted by the second security module if the second security module fails. As such, for this additional reason, Appellants respectfully request that the Board reverse the rejection under Section 103 of claims 33 and 34, and indicate the claims as being allowable.

Conclusion

Appellants respectfully submit that all pending claims are in condition for allowance. However, if the Examiner or Board wishes to resolve any other issues by way of a telephone conference, the Examiner or Board is kindly invited to contact the undersigned attorney at the telephone number indicated below.

Respectfully submitted,

Date: February 20, 2008

Michael G. Fletcher
Reg. No. 32,777
FLETCHER YODER
P.O. Box 692289
Houston, TX 77269-2289
(281) 970-4545

8. APPENDIX OF CLAIMS ON APPEAL

Listing of Claims:

1. A method of operating a first security module in a computer, the method comprising the acts of:

detecting a second security module in the computer, wherein the second security module is configured to perform the same functions as the first security module;

determining whether a key associated with the second security module is stored at the first security module; and

obtaining the key associated with the second security module if the key associated with the second security module is not stored at the first security module.

2. The method set forth in claim 1, wherein each of the first security module and the second security module comprises a trusted platform module ("TPM").

3. The method set forth in claim 1, comprising the act of requesting the key from the second security module.

4. The method set forth in claim 1, comprising the act of sending a public key from the first security module to the second security module if the key associated with the second security module is not stored at the first security module.

5. The method set forth in claim 1, comprising the act of sending a public key along with validation information from the first security module to the second security module if the key associated with the second security module is not stored at the first security module.

6. The method set forth in claim 1, comprising the act of storing the key in a memory associated with the first security module.

7. The method set forth in claim 1, wherein the key is a private key.

8. A first security module in a computer, comprising:

a detector that is adapted to detect another security module configured to perform the same functions as the first security module in the computer and determine whether one of a plurality of keys stored at the first security module is associated with the other security module; and

a device that obtains at least one key associated with the other security module if the one of the plurality of keys stored at the first security module is not associated with the other security module.

9. The first security module set forth in claim 8, wherein the first security module comprises a trusted platform module ("TPM").

10. The first security module set forth in claim 8, wherein the first security module is adapted to request the at least one key from the other security module.

11. The first security module set forth in claim 8, wherein the first security module is adapted to send a public key to the other security module if the at least one key is not stored at the first security module.

12. The first security module set forth in claim 8, wherein the first security module is adapted to send a public key along with validation information to the other security module if the at least one key is not stored at the first security module.

13. The first security module set forth in claim 8, wherein the at least one key is a private key.

14. A first security module in a computer, comprising:

means for detecting another security module in the computer, wherein the other security module is configured to perform the same functions as the first security module;

means for determining whether a key associated with the other security module is stored at the first security module; and

means for obtaining the key associated with the other security module if the key associated with the other security module is not stored at the first security module.

15. The first security module set forth in claim 14, wherein the first security module comprises a trusted platform module ("TPM").

16. The first security module set forth in claim 14, wherein the first security module is adapted to request the key from the other security module.

17. The first security module set forth in claim 14, wherein the first security module is adapted to send a public key to the other security module if the key associated with the other security module is not stored at the first security module.

18. The first security module set forth in claim 14, wherein the first security module is adapted to send a public key along with validation information to the other security module if the key associated with the other security module is not stored at the first security module.

19. The first security module set forth in claim 14, wherein the first security module is adapted to store the key in a memory associated with the first security module.

20. The first security module set forth in claim 14, wherein the key comprises a private key.

21. A computer comprising:

a processor configured to execute program instructions;

a storage device configured to store program instructions to be delivered to the processor;

a first security module; and

a second security module, wherein the second security module is configured to perform the same functions as the first security module, the first security module comprising:

a detector adapted to detect the second security module and determine whether one of a plurality of keys stored at the first security module is associated with the second security module, wherein the first security module obtains at least one key associated with the second security module if one of the plurality of keys stored at the first security module is not associated with the second security module.

22. The computer set forth in claim 21, wherein each of the first security module and the second security module comprises a trusted platform module ("TPM").

23. The computer set forth in claim 21, wherein the first security module is adapted to request the at least one key from the second security module.

24. The computer set forth in claim 21, wherein the first security module is adapted to send a public key to the second security module if the at least one key is not stored at the first security module.

25. The computer set forth in claim 21, wherein the first security module is adapted to send a public key along with validation information to the second security module if the at least one key is not stored at the first security module.

26. The computer set forth in claim 21, wherein the at least one key is a private key.

27. A method of unsealing information from a plurality of security modules, the method comprising the acts of:

detaching an identifier from sealed information for one of the plurality of security modules;

decrypting the sealed information with a key that is associated with another of the plurality of security modules;

calculating a hash of the decrypted sealed information; and

comparing the calculated hash to the identifier to determine if the key was used to encrypt the sealed information;

returning a decrypt key found message if the key is the key used to encrypt the sealed information or returning a decrypt key not found message if the key is not the key used to encrypt the sealed information.

28. The method set forth in claim 27, wherein the plurality of security modules comprise trusted platform modules ("TPMs").

31. A computer network, comprising:

a plurality of computers;

a network infrastructure that connects the plurality of computers together;

at least one of the plurality of computers comprising:

a first security module; and

a second security module, wherein the second security module is configured to perform the same functions as the first security module, the first security module comprising:

a detector adapted to detect the second security module and determine whether a key associated with the second security module is stored at the first security module, wherein the first security module obtains the key associated with the second security module if the key associated with the second security module is not stored at the first security module.

32. The computer network, as set forth in claim 31, wherein each of the first security module and the second security module comprises a trusted platform module ("TPM").

33. The method set forth in claim 1, comprising the act of accessing data encrypted by the second security module using the key associated with the second security module if the second security module fails.

34. The first security module set forth in claim 8, wherein the first security module is configured to decrypt data encrypted by the other security module if the other security module fails.

9. EVIDENCE APPENDIX

None.

10. RELATED PROCEEDINGS APPENDIX

None.